

Implementing Directories

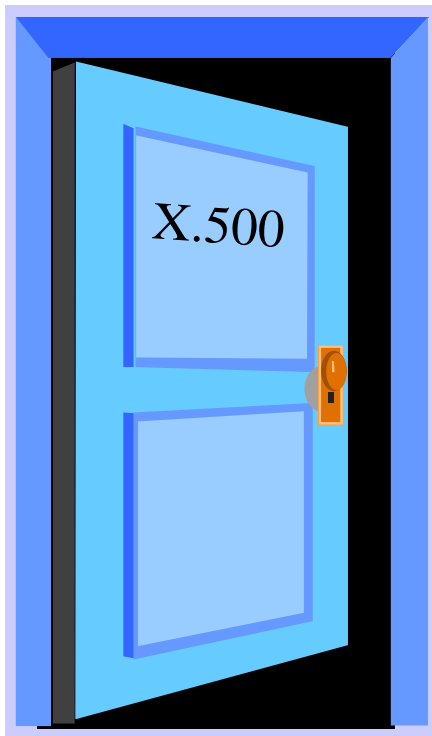
Laura Boyer
J.G. Van Dyke & Associates, Inc..
e-mail: lkf@jgvandyke.com

J.G. Van Dyke & Associates, Inc.
People Making Information Technology Work Securely



Directory Services

The Directory is the key organizational component for information management!



Greet them at the door by integrating all aspects of an organizations workflow:

- Security
- Desktop Applications
- Personnel
- User Capabilities
- Database Integration
- WEB integration

J.G. Van Dyke & Associates, Inc.
People Making Information Technology Work Securely



Directory Process



J.G. Van Dyke & Associates, Inc.
People Making Information Technology Work Securely



Product Selection Criteria

- **Vendor Corporate Viability**
- **Functionality of Product (meets requirements)**
- **Interoperability with other Directories (X.500/LDAP/Web)**
- **Security Capabilities**
- **Performance**
- **Price**
- **Management and Maintainability**
- **Scalability**



Directory Design Considerations

- **Identify the Authoritative Source for Data**
- **DIT Mapping to Directory Management Domains**
- **Naming Issues (Uniqueness)**
- **Defining Access Control Permissions**
- **Use of Replication using Shadowing**
- **Chaining -vs- Shadowing**
- **Security Policies (Authentication, Guards/Firewalls)**
- **Information Storage Issues (sensitive data)**
- **Directory Synchronization**
- **Transition Strategies (Legacy to Future)**
- **System Management/Reporting**



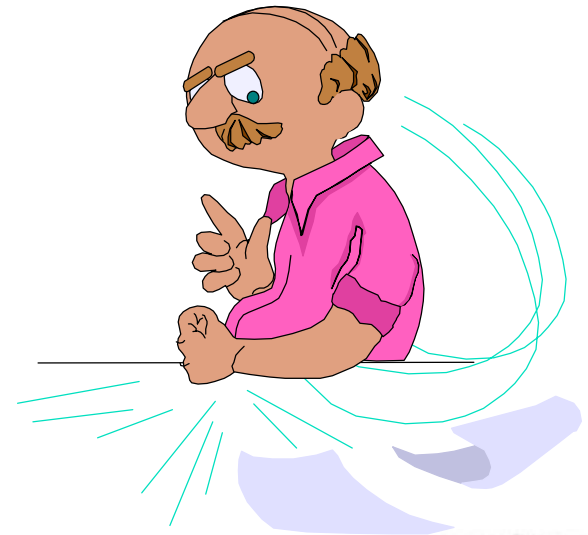
Design Considerations Continued

- **Local Caching Requirements**
- **Establish Knowledge References**
- **Backup/Recovery Strategies**
- **Host/Tenant/Integree Directory Support**
- **Interoperability with Allies**
- **Interoperability with other agencies**
- **Schema Considerations**
- **Platform Considerations/Requirements**



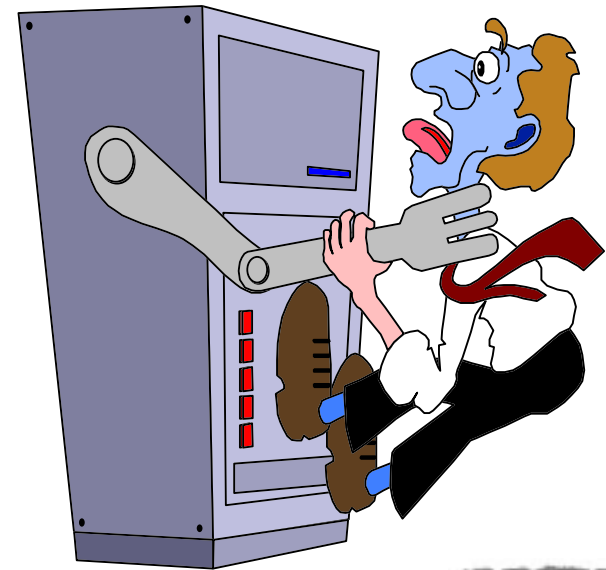
Vendor Interoperability Issues

- **Protocols Supported (LDAP/X.500/Versions)**
- **ASN.1 BER -vs- DER (need to preserve the encoding)**
- **Replication/Shadowing Problems**
- **Performance issues**
- **Interpretation of the Standards**
- **Lack of Security Implementations**
- **Lack of Management Tools**
- **Establishing Trust between vendors**



Shadowing Problems

- Immaturity of 93 shadowing capabilities
- No support for DOP, complexity of configuration
- Little/No Interoperability among vendors
- Ambiguity of Standards (everything is optional)
- X.500 provides tremendous capabilities, vendors did not implement the entire standard
- Known vendor problems:
 - number of shadowing agreements
 - push/pull capabilities
 - sub-tree refinement
 - secondary shadowing
 - incremental shadowing upon change
 - empty DIT limitations
 - time required to shadow data-



Directory Security Issues

- **Time Synchronization**
- **Hardware-Based -vs- Software-Based**
- **Implementing Security at which Layer in the Protocol**
- **Validity Periods**
- **Cross-Certification**
- **Multiple Certificates under one DN vs. Separate Entries**
- **Guards/Firewalls**
- **Verifying Authorizations/Personality Needs**
- **Multiple Digital Signature/Encryption Algorithms**
- **Certificate Validation Process**
- **Certificate Revocation Process**

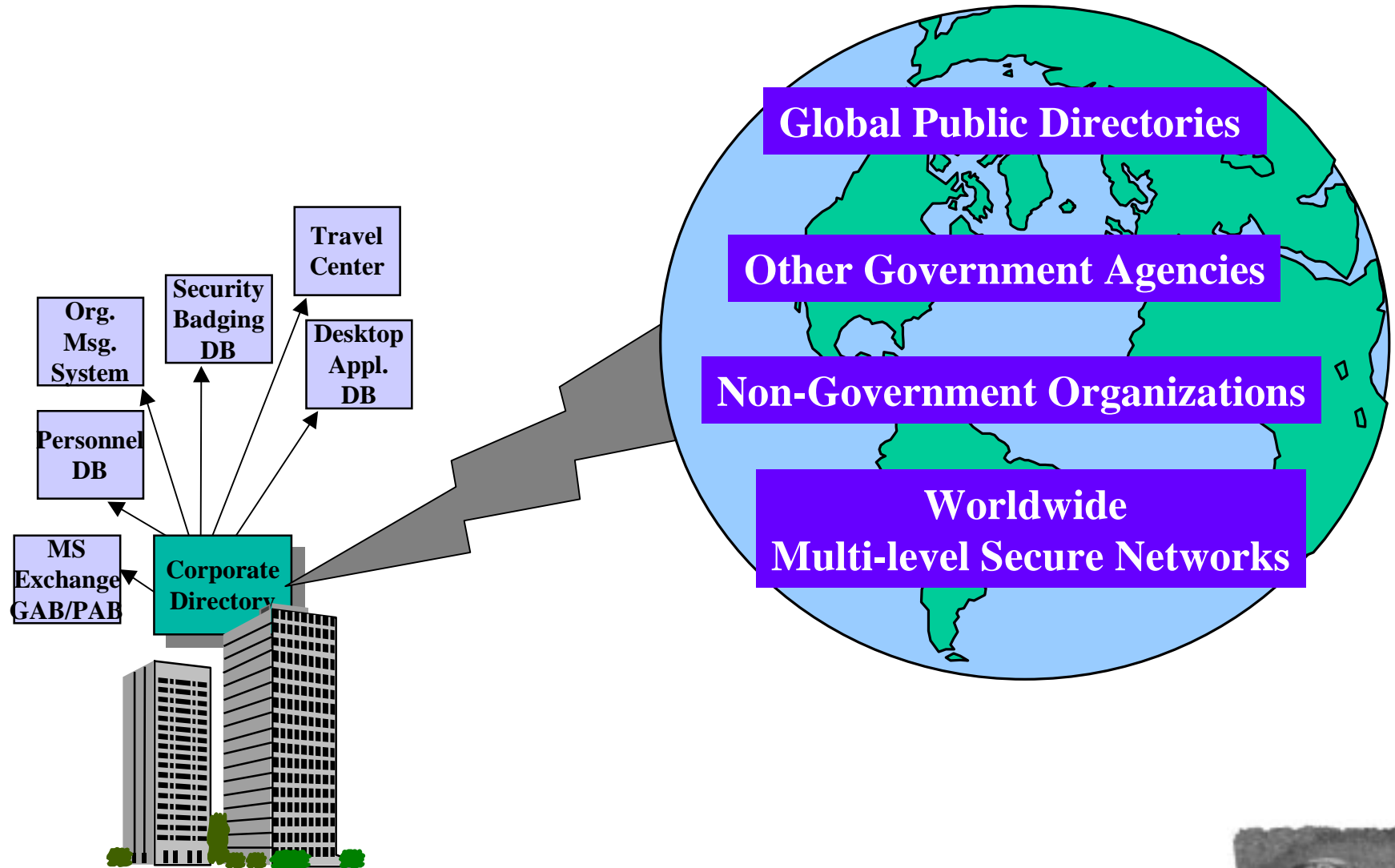


Security Issues Continued

- **Using Certificate for Authentication**
Purposes only not for authorizations and privilege.
- **X.509 -vs- Proprietary Certificate formats**
- **Support for Multiple Types of Certificates**
- **Increase in entry size**
- **Archive**
- **Data Recovery**



Summary



J.G. Van Dyke & Associates, Inc.
People Making Information Technology Work Securely

